## Remarks

### *A. Status of Application*

Claims 11-21 were pending. Claim 11 has been amended to include the limitations of claims 17 and 18. Accordingly, claims 17 and 18 have been canceled. No new matter has been added.

Claims 11-16 and 21 were rejected under 35 U.S.C. §103(a) as being unpatentable over Elliott (Building the quantum network) in view Buer et al. (US 20040005061). Claims 17 and 18 were rejected under 35 U.S.C. §103(a) as being unpatentable over Elliot in view of Buer in further view of Elliot (US 7457416), claim 19 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Elliot in view of Menezes, et al, *Handbook of Applied Cryptography* (hereinafter "Menezes"), and claim 20 was rejected 35 U.S.C. §103(a) as being unpatentable over Elliott in view of U.S. Patent No. 5,850,441 to Townsend et al. (hereinafter "Townsend").

### *B. Summary of Examiner Interview*

Applicant thanks the Examiner for his time and consideration in discussing the present application in the Examiner interview held Tuesday, March 30, 2010. During the course of the interview, the Examiner suggested amending claim 18 into independent form and indicated that claim 18 is allowable over the art of record.

### *C. The Rejections Under 35 U.S.C. §103 are Overcome*

#### 1. Rejection of Claim 11 is Overcome

Claims 11-16 and 21 were rejected under 35 U.S.C. §103(a) as being unpatentable over Elliott (Building the quantum network) in view Buer et al. (US 20040005061).

Amended Claim 11 reads:

> 11. A communication system using quantum cryptography comprising:
>
> subscriber stations connected to one or more quantum channels;
>
> one or more quantum-cryptographic device associated with the one or more quantum channels for generating a quantum key during use; and

two or more interconnected switching stations that, during use, communicate via **first public lines**, using encryption agreed upon, without quantum-cryptographic key exchange;

wherein, during use, the subscriber stations are connected to the switching stations via the one or more quantum channels that generate a respective temporary quantum key and are adapted to communicate via **second public** lines using the quantum key, and **wherein the first public lines are distinct from the second public lines, and are a priori secure lines to transmit the generated quantum key from one switching station to another and to another subscriber station;**

**wherein the subscriber stations involved in a given communication generate a separate key bit sequence with their associated switching station via the quantum channel after a request for a communication has been transmitted via a respective switching station during use; and**

**wherein, during use, a switching station associated with a called subscriber station generates a third key bit sequence from the key bit sequences generated via the quantum channels and transmits this third key bit sequence to the called subscriber station which, using the key bit sequence known to it and generated by it together with the associated switching station, from the third key bit sequence generates the key bit sequence generated on the part of the calling subscriber station, which then finally is used as a mutual key for the communication between the subscriber stations.**

*Claim 11* (emphasis added).

Amended claim 11 includes elements of claims 17 and 18. During the Examiner interview of March 30, 2010, the Examiner indicated that claim 18 would be allowable if rewritten in independent form. Therefore, claim 11 in its amended form is allowable, because amended claim 11 includes all of the elements of claims 17 and 18.

(a) Elements of Claims 17 and 18 are Allowable in Independent Form

The Action asserts that "Elliott et al. discloses generating key bits between subscriber stations and their associated switching stations after a request for communication has been transmitted." Applicants respectfully disagree.

During the interview, the Examiner acknowledged that these elements would be allowable if rewritten in independent form. Additionally, the Action acknowledges that Elliot '091 fails to disclose "generating a separate bit sequence and wherein, during use, a switching station associated with a called subscriber station generates a third key bit sequence from the key bit sequences generated via the quantum channels and transmits this third key bit sequence to the called subscriber station which, using the key bit sequence known to it and generated by it together with the associated switching station, from the third key bit sequence generates the key bit sequence generated on the part of the calling subscriber station, which then finally is used as a mutual key for the communication between the subscriber stations." *Id.* The Action asserts that "Elliot ['416] teaches such a quantum key agreement protocol" at Fig. 4 and col. 6, line 48 – col. 7, line 38. Applicant disagrees with this assertion.

"A *prima facie* case of obviousness may [] be rebutted by showing that the art, in any material respect, teaches away from the claimed invention." MPEP 2144.05(III) (quoting In re Geisler, 116 F.3d 1465, 1471 (Fed. Cir. 1997)).

The cited portion of Elliot '416 actually teaches away from claims 17 and 18 to the extent that they are included in claim 11. Specifically, Elliot '416 describes a system where endpoints each send QC keys to respective KDC devices. The KDC devices then exchange the QC keys and establish one of the exchanged keys as a common key. Col. 7, lines 1-32. Thus, Elliot '416 explicitly teaches away from claim 11 by teaching that switching devices should exchange quantum cryptographic keys, whereas claim 11 describes a system wherein "two or more interconnected switching stations that, during use, communicate via first public lines, **using encryption agreed upon, without quantum-cryptographic key exchange.**" Therefore, amended claim 11 is allowable, because it has been amended to include the allowable features of claims 17 and 18.

(b) Additional Features of claim 11 are Patentable

Additionally, Applicant asserts that the combination of Elliot '091 and Buer fails to disclose other features of Claim 11. In particular, the combination fails to teach a

communication system "wherein the first public lines are distinct from the second public lines, and are a priori secure lines to transmit the generated quantum key from one switching station to another and to another subscriber station" as recited in claim 11.

Elliot '091 describes a quantum cryptographic network (QC-network) 105 which includes a plurality of routers and hosts interconnected via links 552-578 which form single nodes in this network. *See* Elliot '091, Fig. 5. Some of the links 552-578 are protected by quantum cryptographic techniques (illustrated by solid lines in Fig. 5), while others are unprotected (illustrated by dashed lines in Fig. 5). Accordingly, for end-to-end message transmission between a source host 535 and a destination node according to Elliot '091 (e.g., description in connection with Figs. 17-20), the message to be sent is to be provided with a header which specifies both the required security level of the transmission and the address of the destination node. When a certain hop node receives the message, the destination address contained in the message header is compared with the address assigned to the hop node in order to determine if the message has already reached its destination node. If not, the message is passed to the next hop node by means of a forwarding table 725 and QC-Interface (QCLI). The QC-Interface then exchanges quantum cryptographic keys with the next hop node. Col. 11, lines 4-13.

Elliott '091 nowhere disclose a communication system, where distinct first and second public lines interconnect switching stations and subscriber stations, respectively, wherein the first public lines are a priori secure public lines.

Elliott '091 merely teach a communication network having mixed quantum cryptographically secured lines and unprotected lines (illustrated by solid lines and dashed lines, respectively, in figure 5) for concatenating short communication distances hop node by hop node. As can be clearly seen from Fig. 5 of Elliott '091, therein no distinction is made between first and second public lines. In particular, there is no direct connection between two hosts (cf. hosts 535, 540, 545, 550 in Fig. 5) via public lines distinct from quantum channels connecting the hosts to the routers and public lines interconnecting the routers. Also, nowhere from the specification or the figures can it be inferred that different types of public lines - a priori secure lines for interconnecting the routers and regular public lines for interconnecting the hosts - are contemplated.

By contrast, claim 11 describes "two or more interconnected switching stations that, during use, communicate via first public lines, **using encryption agreed upon, without**

**quantum-cryptographic key exchange.**" Elliot '091 discloses a system where two or more interconnected routers communicate via quantum cryptographic lines by exchanging quantum cryptographic keys, but this system does not provide the advantages of a communication system "wherein the first public lines are distinct from the second public lines, and are a priori secure lines to transmit the generated quantum key from one switching station to another and to another subscriber station," as described in claim 11.

Indeed, the Office admits that Elliot '091 fails to teach this limitation of claim 11, but cites Buer in support of the rejection under 35 U.S.C. § 103. Applicants respectfully assert that Buer also fails to teach the recited element of claim 11.

Buer teaches an encryption key management system for providing secured data transmission and for managing cryptographic keys. Buer does not, however, teach a system "wherein, during use, the subscriber stations are connected to the switching stations via the one or more quantum channels that generate a respective temporary quantum key and are adapted to communicate via second public lines using the quantum key, and wherein the first public lines are distinct from the second public lines, and are a priori secure lines to transmit the generated quantum key from one switching station to another and to another subscriber station," as recited in claim 11. First, Buer makes no mention of quantum cryptogrophy or quantum cryptographic keys. Second, it appears that Buer fails to teach a system wherein switching stations communicate via first public lines and second public lines, "wherein the first public lines are distinct from the second public lines, and are a priori secure lines to transmit the generated quantum key from one switching station to another and to another subscriber station," as recited in claim 11. Indeed, it does not appear that Buer makes any mention of switching stations having distinct public lines or that any of the public lines are a prior secure. Additionally, it appears that Buer fails to teach "transmit[ting] the generated quantum key from one switching station to another and to another subscriber station," as recited in claim 11.

Therefore, the combination of Elliot '091 and Buer fails to teach every element of amended claim 11, and the rejection under 35 U.S.C. § 103 is overcome. Applicant asserts that dependent claims 12-21 are also allowable because of their dependence on allowable independent claim 11. *See* In re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988).

### 2. Rejection of Claim 19 is Overcome

Claim 19 was rejected under 35 U.S.C. §103(a) as being unpatentable over Elliott '091 in view of Menezes, et al. The rejection is overcome because claim 19 depends upon allowable claim 11. Nevertheless, Applicant traverses the rejections.

The Action acknowledges that "Elliot et al. fails to explicitly disclose discarding the quantum keys at the end of a communication." Nonetheless, the Office points to Menezes to support the rejection. Applicant disagrees with the Office's characterization of Menezes. More specifically, the cited portion of Menezes teaches cryptoperiods, long-term keys, and short-term keys. Menezes defines a "cryptoperiod" of a key as "the time period over which it is valid for use by legitimate parties." Menezes, at pg. 553. Similarly, "short-term keys" are described as keys "often used as data keys or *session keys* for a single communication session." By contrast, claim 19 recites a communication "wherein, during use, quantum keys generated for a given communication are discarded at the end of the communication." Thus, according to claim 19, the trigger for discarding the quantum keys is the "end of the communication" not the expiration of some arbitrary time period or termination of a full communication session as disclosed by Menezes. Thus, claim 19 is patentable over the combination of Elliot '091 and Menezes, because the combination fails to teach every element of claim 19.

## Conclusion

In light of the presented remarks, Applicant assert that Claims 11-16, and 19-21, with the current amendments, are patentable and in condition for prompt allowance. Should additional information be required, the Examiner is respectfully asked to notify Applicants of such need. If any impediments to the prompt allowance of the claims can be resolved by a telephone interview, the Examiner is respectfully requested to contact the undersigned.

Respectfully submitted,

Mark B. Wilson, Reg. No. 37259
for S. Scott Gordon
Reg. No. 57,294
Attorney for Applicant

FULBRIGHT & JAWORSKI L.L.P.
600 Congress Avenue, Suite 2400
Austin, Texas 78701
Telephone: (512)536-3018
Facsimile: (512) 536-4598

Date: April 15, 2010